CPA
Practice Advisor

ACCOUNTING

WISP Required! Key Components in Your Firm's Written Information Security Plan

While primarily targeted at companies maintaining more than 5,000 client records (think tax returns), certain safeguard components are required for firms with fewer than 5,000 records.

Roman Kepczyk • Jun. 14, 2023

While the FTC Safeguards rule designed to protect financial and PII (personally identifiable information) has been around for decades, as of June 9, 2023, compliance of various components including a Written Information Security Plan, or WISP, became mandatory! While primarily targeted at companies maintaining greater than 5,000 client records (think tax returns), certain safeguard components are required for firms with fewer than 5,000 records, such as the use of multi-factor authentication, encryption of data, and secure disposal of Information.

Also, with financial and criminal penalties imposed for "knowingly or inadvertently" disclosing taxpayer data, the IRS has issued additional guidance on key strategies for protecting taxpayer data which would apply to all firms regardless of the number of clients they have. The need for a WISP was highlighted for practitioners when they renewed their PTIN and expanded requirements including security and phishing training. Accordingly, it is recommended that all firms have a WISP with the caveat that it is "appropriate" to their firm's size and situation. Below we identify key components that should be documented in writing to be incorporated into firm WISPs as well as templates and resources to help you get started.

STEP 1: Designate WISP Leader: Firm's must appoint an individual to represent the firm in coordinating the development of the firm's information security program. This includes providing the authority to hire security consultants, external technical expertise, and work with knowledgeable service providers to assist with the technical components which are most likely beyond the technical knowledge and understanding of the WISP leader.

STEP 2: Conduct a Risk Assessment: The firm must identify where all protected data is located and how it may be utilized including the foreseeable cybersecurity risks and system vulnerabilities that could compromise this data. This can begin by listing all the firm's applications and identifying which contain protected data as well as the location where this data is stored, whether on individual hard drives, mobile media, firm network drives, or in the cloud (hosted applications and data backup providers).

The same stringent risk assessment procedures the firm applies to its internal systems should be applied to third-party cloud application vendors and hosting providers. This comprehensive file inventory should also indicate if that data is encrypted and who has access to these files (regularly checking to verify that individual access is terminated when the employee or contractor is terminated).

STEP 3: Implement Safeguards: The next step is to identify the safeguards the firm has in place and whether they are deemed adequate. Right Networks has coined the phrase "Smart Security Management" to separate CPA firm safeguards into three components: Securing Firm/Client Data, Protecting User Access, and Ongoing Cyber Education.

Firms should partner with IT experts and cloud providers to implement "Enterprise" grade cybersecurity solutions including intrusion detection, prevention, and remediation as well as a "hardened" IT infrastructure to ensure system resilience and business continuity. This would entail automatic updating of the operating systems and firmware for all computing and network devices including remote users and home Wi-Fi. Preventing unlawful access is the second component and includes the use of multi-factor authentication, complex passwords (12+ characters recommended), and technical solutions to ensure passwords are unique and not re-used (such as password wallets to store them).

The final component of Smart Security Management is employee education discussed in Step 5. To assist firms in identifying current IT safeguards and security best practices, Right Networks has a Cybersecurity Checklist available at: CPA-

Cybersecurity-Checklist.pdf (rightnetworks.com) which was originally created for the AICPA PCPS. The WISP leader should walk through this listing with their IT experts at least annually so they understand the firm's status on each item and can implement safeguards where needed.

STEP 4: Ongoing Testing and Monitoring: The WISP leader must work closely with their internal IT personnel and external security contractors to ensure that cyber safeguards are being continuously monitored and that alerts are being followed up with and remediated. Special attention should be given when new applications or hardware are implemented to ensure that they fall within the WISP guidelines and do not expose firm data to unintended consequences. Data backups should be tested regularly as well as disaster recovery solutions to ensure the firm can recover from a breach or ransomware event.

STEP 5: Employee Education: The IRS recommends firms provide ongoing cyber security education discussing not only the firm's security policies and procedures, but also education on current and evolving threats, how to connect securely via a VPN (virtual private network), and how to respond in the event the employee suspects a breach. Firm policies regarding client data should be reviewed and updated annually such as for example the firm's document retention policy where personnel should be educated on how to properly delete files (including that which is stored on external media).

Security training would also include regular updates on how cybercriminals are using social engineering and increasingly sophisticated phishing email schemes to get firm members to provide information, allow malicious access, and to unintentionally click on a link or download files and applications that may contain malware.

STEP 6: Preparing for the Worst: Additional components of the WISP include having a breach response plan and cyber-insurance in place in the event of a breach. The breach response team should include expertise in responding to and remediating a cyber event and a plan to communicate with the appropriate authorities and any impacted clients. Insurance policies should also be reviewed annually to ensure that any new requirements are being covered as well as verifying the firm has adequate 1st and 3rd party coverage if the firm is breached.

As outlined in the steps above, it's obvious that developing a WISP is a significant undertaking but it is one that if done properly will better protect the firm and its client's data. To assist firms in formalizing their WISP, the IRS provides a template

via Publication 5708: How to Create a Written Information Security Plan for Your Tax & Accounting Practice.

———-

Roman H. Kepczyk, CPA.CITP, CGMA is director of Firm Technology Strategy for Right Networks and partners exclusively with accounting firms on production automation, application optimization and practice transformation. He has been consistently listed as one of INSIDE Public Accounting's Most Recommended Consultants, Accounting Today's Top 100 Most Influential People, and CPA Practice Advisor's Top Thought Leaders.

Accounting • Firm Management • Hardware • IRS • Security • Taxes • Technology

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.